www.umercs.com January 2026

uMercs Cybersecurity News Digest

Insider Tips for Boosting Cybersecurity and Streamlining Business Efficiency

CYBERSECURITY BLIND SPOTS:

THE RISKS YOU DON'T SEE BUT HACKERS DO

Every business leader understands the importance of cybersecurity. Yet the biggest threats often aren't headline-grabbing breaches. They're the overlooked gaps hiding in plain sight. These blind spots may seem minor: a missed software update, an inactive account or an untested backup. But for hackers, they're open doors. Here are the most common gaps and how to close them before they become costly mistakes:

1. Unpatched systems

Every missed update is an invitation to attackers. Hackers track patch cycles and exploit known vulnerabilities.

Fix: Automate patch management and set alerts for lagging systems.

2. Shadow IT and rogue devices

Employees downloading unauthorized apps or connecting personal devices to your network can introduce malware that stays dormant until it's too late.

Fix: Enforce strict app and device policies. Regularly scan for unknown endpoints.

3. Over-permissive access

Too much access is dangerous. Hackers love accounts with excessive permissions.

Fix: Apply least privilege principles, mandate MFA and review permissions regularly.

4. Outdated security tools

Cyberthreats evolve daily. Old antivirus or intrusion detection tools can't keep up.

Fix: Audit your security stack and replace outdated tools before they fail you.

5. Orphaned accounts

Former employees' credentials often remain active, making them prime targets for attackers.

Fix: Automate offboarding to disable accounts immediately.

6. Misconfigured firewalls

A firewall is only as strong as its settings. Old or temporary rules create vulnerabilities.

Fix: Audit configurations, document changes and remove unnecessary permissions.

7. Untested backups

Backups aren't a safety net unless they work. Many businesses discover too late that theirs are corrupt or incomplete.

Fix: Test backups quarterly and store them securely in immutable storage.

8. Missing security monitoring

You can't protect what you can't see. Without centralized visibility, threats slip through unnoticed.

Fix: Invest in continuous monitoring or partner with an experienced IT provider.

9. Compliance gaps

Frameworks like GDPR or HIPAA aren't just paperwork. They're essential for strong security.

Fix: Conduct regular compliance reviews and maintain documentation.

Bottom line: Identifying blind spots is only the beginning. The real value lies in fixing them quickly. Start with these fixes and you'll strengthen your defenses where it matters most.

uMercs Cybersecurity News Digest

SoundCloud confirms breach after member data stolen, VPN access disrupted

Overview

SoundCloud confirmed a security breach where threat actors, reportedly the ShinyHunters extortion gang, accessed an ancillary service dashboard and stole a database exposing email addresses and public profile info for ~20% of users (roughly 28 million accounts). No sensitive data like passwords or financial info was compromised. The breach caused VPN connection issues (403 errors) due to SoundCloud's response measures and follow-on denial-of-service (DoS) attacks. SoundCloud investigated, blocked access, enhanced monitoring/access controls, and worked with experts, but VPN disruptions persist.

How a Penetration Test Could Have Prevented This Breach

Penetration testing (pen testing) simulates real-world attacks to identify vulnerabilities before exploitation. Here, it could have:

Detected dashboard misconfiguration: Testers likely would have uncovered weak access controls on the "ancillary service dashboard," a common entry point for breaches (e.g., via exposed APIs or insufficient authentication).

Exposed unauthorized access paths: Red-team exercises could reveal lateral movement opportunities, preventing initial foothold.

Validated incident response: Pre-breach pen tests often include purple-team simulations, improving detection speed and reducing fallout like VPN blocks or DoS vulnerability.

Evidence: Similar breaches (e.g., ShinyHunters' PornHub attack) stem from untested admin panels; pen tests at firms like Wiz (mentioned) routinely flag these, as per industry reports from Krebs on Security and MITRE ATTACK frameworks.

Credential Vulnerabilities

The article states no password data was stolen, but the breach highlights potential credential risks:

- **Weak or default creds on dashboards**: Attackers likely used compromised/stolen creds or no MFA for the ancillary service, a top vector per Verizon's 2024 DBIR (81% of breaches involve weak creds).
- **No evidence of credential stuffing**: Public profiles reduced impact, but exposed emails enable phishing for creds.
- **ShinyHunters pattern**: This group often exploits leaked creds from prior breaches (e.g., via HaveIBeenPwned databases) for initial access.

Mitigation gap: SoundCloud's post-breach review of "identity and access controls" implies prior lapses like shared or unrotated creds.

Storage Securities

Issues centered on database exposure rather than core storage:

- **Ancillary database isolation failure**: The stolen DB was "limited" but held 28M records; poor segmentation allowed access without hitting sensitive storage.
- **Public data overlap**: Emails/profiles were already public, minimizing damage, but storage lacked encryption-at-rest or access logging.
- **Response-induced issues**: Config changes blocked breaches but broke VPNs, suggesting insecure storage of IP rules or WAF configs.

Best practices violated: NIST SP 800-53 requires least-privilege access and query logging; a secured setup (e.g., AWS RDS with IAM) would log/audit the access, enabling faster detection.

Overall Takeaways

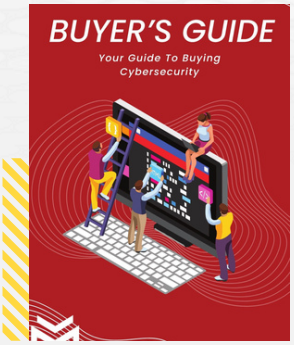
- **Scope downplays risk**: "Limited" data still affects 28M users; exposed emails fuel phishing/extortion (ShinyHunters' MO).
- **Response trade-offs**: Quick blocking prevented escalation but caused outages/DoS bait—balance security with availability.
- **Proactive measures work**: Post-breach hardening (monitoring, access reviews) is good, but pen tests and zero-trust architecture prevent repeats.
- **Industry trend**: ShinyHunters targets media platforms (SoundCloud, PornHub); firms should prioritize third-party dashboard security, MFA everywhere, and regular audits.

Key stat: IBM's 2024 report shows breaches cost $4.88M avg.—prevention via pen testing yields 6x ROI per Ponemon Institute. SoundCloud's transparency is a plus, but full disclosure on root cause would aid peers.

Source: BleepingComputer
SoundCloud confirms breach after member data stolen, VPN access disrupted
https://www.bleepingcomputer.com/news/security/soundcloud-confirms-breach-after-member-data-stolen-vpn-access-disrupted/?&web_view=true

BUYER'S GUIDE

What Every Small-Business Owner Must Know About Purchasing And Protecting Their Company's Critical Data



When exploring cybersecurity solutions with Uncommon Mercenaries (uMercs), focus on these key areas:

Penetration Testing: uMercs offers expert penetration testing to identify vulnerabilities by simulating real-world attacks. Look for their certifications and methodologies to ensure they provide thorough assessments and actionable insights.

Market Pricing: uMercs provides competitive pricing tailored to your organization's needs. Compare their pricing models with industry standards to ensure transparency and value, avoiding hidden costs.

Monitoring and Maintenance: Cybersecurity requires ongoing effort. uMercs delivers continuous monitoring, incident response, and regular updates to keep your defenses strong against evolving threats. Evaluate their monitoring frequency and support responsiveness to ensure effective protection.

By considering these aspects, you can confidently choose uMercs as your cybersecurity partner, safeguarding your organization against cyber threats.

Claim Your FREE Copy Today At www.umercs.com

CARTOON OF THE MONTH

"The look you get when you say, 'Let's circle back.'"